

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA,

-against-

MEMORANDUM AND ORDER  
18-CR-0349(S-1) (JS) (AKT)

LORRAINE CHALAVOUTIS,

Defendant.

-----X

APPEARANCES

For the Government: Charles Peter Kelly, Esq.  
United States Attorney's Office  
Eastern District of New York  
610 Federal Plaza  
Central Islip, New York 11722

For the Defendant: Bruce A. Barket, Esq.  
Alexander R. Klein, Esq.  
Kevin T. Kearon, Esq.  
Barket Marion Epstein & Kearon LLP  
666 Old Country Road, Suite 700  
Garden City, New York 11530

SEYBERT, District Judge:

Defendant Lorraine Chalavoutis ("Defendant" or "Chalavoutis") moves for (1) dismissal of the Aggravated Identity Theft charges (Counts Six and Seven) in the Superseding Indictment pursuant to Rule 12(b)(3) of the Federal Rules of Criminal Procedure; (2) judicial review of the grand jury minutes; and (3) contravention of the search warrant. (Def. Mot., D.E. 81.) The Government opposes Defendant's motion in its entirety. (Gov't Opp., D.E. 87.) The Court heard oral argument on the motion on

November 22, 2019. (Nov. 22, 2019 Minute Entry, D.E. 90.) For the following reasons, Defendant's motion is DENIED.

#### BACKGROUND

Chalavoutis is charged with Conspiracy to Commit Mail Fraud in violation of 18 U.S.C. §§ 1349 and 3551 et seq. (Count One); Mail Fraud in violation of 18 U.S.C. §§ 1341, 2, and 3551 et seq. (Counts Two, Three, Four, and Five); Conspiracy to Commit Money Laundering in violation of 18 U.S.C. §§ 1956(h), 1956(a)(1), 1957(b) and 3551 et seq. (Count Eight); Money Laundering in violation of 18 U.S.C. §§ 1957(a), 1957(b), 2, and 3551 et seq. (Count Nine); and, most relevant here, Aggravated Identity Theft ("AIT") in violation of 18 U.S.C. §§ 1028A(a)(1), 1028A(b), 1028A(c)(5), 2, and 3551 et seq. (Counts Six and Seven). (See Superseding Indictment ("SI") D.E. 73, ¶¶ 14-25.)

#### I. The Charges

As charged, Chalavoutis worked with co-conspirators Tully Lovisa and Shaun Sullivan (both of whom have pled guilty)<sup>1</sup> to perpetuate a large direct mail fraud against thousands of mostly "elderly and vulnerable" victims. (SI ¶¶ 1, 3.) Essentially, defendants sent prize-promotion mail to victims, indicating that the victims would receive cash prizes if they paid a small fee--

---

<sup>1</sup> On October 12, 2018, Lovisa pled guilty to conspiracy to commit mail fraud and wire fraud. (D.E. 47.) On May 14, 2019, Sullivan pled guilty to conspiracy to commit mail fraud. (D.E. 64.)

typically denoted as a "processing" or "delivery" fee. (SI ¶¶ 3, 9.) No victim who sent a fee to defendants ever received a promised payment. (SI ¶ 13.) From December 2010 to July 2016, the defendants received approximately \$30 million from the victims. (SI ¶ 13.)

Lovisa and Sullivan, who ran the direct-mail scheme, paid Chalavoutis for operational services.<sup>2</sup> (SI ¶ 2.) In order to facilitate this operation, defendants used multiple different company names (the "Shell Companies") as purported senders of the promotional mailings (the "Straw Owners"). (SI ¶¶ 1-2.) Chalavoutis used Straw Owners to form the Shell Companies and open accounts with banks and payments processors. She controlled these accounts, and transferred money received from the victims to Lovisa, Sullivan, herself, and others involved in the operation. (SI ¶ 2.)

Chalavoutis was originally charged with Lovisa and Sullivan. (See Indictment, D.E. 1.) After Lovisa and Sullivan

---

<sup>2</sup> Defendant argues that she employed herself as a bookkeeper for many entities on an as-needed basis, and that in 2013 and 2014, less than 10% of her clients had any association with the direct-mail companies in this case. (Def. Br., D.E. 82, at 3.) The Government disagrees with Defendant's minimal description of her role, and puts forth that she was an important participant who controlled the accounts and was "best positioned to know the essential financial facts of the scheme" who also knew that Lovisa had been sued by the Federal Trade Commission and whose companies had been shut down by the United States Postal Service. (Gov't Opp. at 3.)

pled guilty, the Government filed the Superseding Indictment as to Chalavoutis, which "removed counts from the original Indictment that were focused solely or primarily on conduct by other defendants and added two new [AIT] counts (Six and Seven)." (Gov't Opp. at 4.)

The AIT counts charge that Chalavoutis, on or about May 1, 2015 and on or about March 31, 2016, "together with others . . . did knowingly and intentionally transfer, possess and use, without lawful authority, one or more means of identification of another person, to wit: Jane Doe, an individual whose identity is known to the Grand Jury, knowing that the means of identification belonged to another person." (SI ¶¶ 19, 21.) Count Six relates to a corporate annual report Chalavoutis filed with the Florida Secretary of State for one of the Shell Companies in the Superseding Indictment. It identifies the Straw Owner by name and address and is purportedly electronically signed by the Straw Owner. It was actually signed by Chalavoutis. (Gov't Opp. at 5.) Count Seven is based on a check from the same Shell Company to a printer. The check is again purportedly signed by the Straw Owner, but the signature was put on the check by Chalavoutis using a signature stamp. (Gov't Opp. at 5.)

## II. The Search Warrant

Prior to the original Indictment, Judge Anne Y. Shields issued a search warrant for two email accounts used by Chalavoutis.

(See Warrant, Gov't Ex. C, D.E. 81-4, at ECF pp. 76-83 LC 000077.) The Court assumes familiarity with the warrant, but notes that in attachment B3, the warrant describes the "information to be disclosed by the [email provider]" as "[t]he contents of all emails associated with the account" "from October 14, 2010 through December 6, 2016." (Warrant at LC000078.) The "[i]nformation to be seized by the government" is described as "All information . . . that constitutes fruits, contraband, evidence" of certain enumerated crimes, or "violations involving Tully Lovisa, Shaun Sullivan, Faith Carey, Lorraine Chalavoutis, Errol Seales, Casey Stefiuk and their coconspirators including but not limited to PacNet, and any individual or entity receiving services from and/or working in concert with them, and occurring from October 14, 2010 through December 6, 2016, including, for each account or identifier, information pertaining to the following matters," followed by a list of subjects and types of information, including but not limited to customer databases or lists, contracts, correspondence, advertising, legal documents, invoices, business records, and financial records. (Warrant at LC 000080-82.) The warrant also allows the Government to seize "[e]vidence indicating how and when the email account was accessed or used" and "[e]vidence indicating the email account owner's state of mind as it relates to the crimes under investigation." (Warrant at LC 000082-83.)

## DISCUSSION

### I. Motion to Dismiss Counts Six and Seven

Chalavoutis argues that the AIT counts should be dismissed because the Superseding Indictment does not allege that she used other people's means of identification without their consent when creating the Straw Owner Shell Accounts. She "urge[s] th[is] Court to take the minority view" and find that the AIT statute requires a lack of consent of the person whose name was used. (Def. Br., at 1.) The Government responds that although the Second Circuit has not squarely addressed the issue, every other Circuit Court and many district courts--including this one--have taken the position that lack of consent is not required. (Gov't Opp. at 8.)

This Court has previously held that "[b]y its plain text, the [AIT] statute does not require the non-consent of the individual whose identity the defendant transfers, uses, or possesses. Indeed, the case law is well-settled that the key inquiry is whether the defendant used the means of identification of another 'without lawful authority,' and that the consent of the victim has no bearing on that inquiry." United States v. Cwibeker, No. 12-CR-0632, 2015 WL 459315, at \*3 (E.D.N.Y. Feb. 2, 2015) (collecting cases). Another district court in this Circuit noted that "every single Court of Appeals that has considered the issue, except for one, has ruled that § 1028A is violated whenever the

defendant uses another person's identity in furtherance of one of the enumerated crimes, regardless of whether the other person consented to the use. That majority view is shared by the district courts in this Circuit that have ruled on the issue." United States v. Roberts-Rahim, No. 15-CR-0243, 2015 WL 6438674, at \*7 (E.D.N.Y. Oct. 22, 2015) (collecting cases); see also United States v. Naranjo, 645 F. App'x 50, 52 (2d Cir. 2016) ("In this circuit, there is no binding precedent governing the issue of how § 1028A should be interpreted, or whether the government is required to prove that the individuals did not consent to the unlawful use of their identities. The majority of other circuits that have considered the[se] questions . . . have adopted the government's interpretation [that it is not required to demonstrate a lack of consent]") (holding it was not plain error for district court to instruct the jury that the Government had to prove the defendant "used the identification 'without the consent or knowledge of the person' or used 'the identification in furtherance of a crime even with the person's consent'" (emphasis added)); United States v. Gatwas, 910 F. 3d 362, 365 (8th Cir. 2018) (consent "argument has been widely rejected").

Defendant urges the Court to adopt the approach of the Seventh Circuit, the only Court of Appeals to take the contrary position that the AIT statute requires a lack of consent of the person whose identity was used. See Roberts-Rahim, 2015 WL 6438674

at \*8 ("Only the Court of Appeals for the Seventh Circuit seemingly has taken a conflicting position, holding in Spears v. United States [729 F. 3d 753 (7th Cir. 2013)] that § 1028A requires the lack of consent of the person whose identity was used in order to establish a violation."). As it did in Cwibeker, the Court declines to adopt this approach.

Chalavoutis cites Cwibeker and argues that it left open the possibility that under certain factual scenarios, consent of a coconspirator, as opposed to a "victim," could render the AIT statute inapplicable. Chalavoutis contends that the Straw Owners are likely "co-conspirators in the scheme rather than its victims, getting paid for their involvement." (Def. Reply, D.E. 89, at 7.) This Court did note in Cwibeker "[t]he presence of real, ascertainable, and immediate victims" which "render[ed] the core reasoning behind the [Seventh Circuit's] decision in Spears patently inapplicable[.]" Cwibeker, 2015 WL 459315 at \*4. However, regardless of the situation, the statute requires only that a perpetrator uses another person's identity "without lawful authority." 18 U.S.C. § 1028A(1). The majority view is that "consent from another person to use his or her identity does not confer 'lawful authority' upon the defendant to use that identity for an unlawful purpose." Roberts-Rahim, 2015 WL 6438674 at \*7.

United States v. Otuya, 720 F.3d 183 (4th Cir. 2013) is instructive. There, the defendant paid college students "in

exchange for access to their bank account and ATM cards, which the conspirators would then use to process [ ] stolen checks” and defraud banks. Id. at 185. The defendant argued that his AIT conviction should be reversed “because his coconspirator . . . agreed to [the defendant’s] nefarious use of his identification[.]” Id. at 189. The court “reject[ed] this argument for a straightforward reason: no amount of consent from a coconspirator can constitute ‘lawful authority’ to engage in the kind of deplorable conduct that [the defendant] engaged in [and s]imply put, one does not have ‘lawful authority’ to consent to the commission of an unlawful act.” Id. Further, “[t]o excuse [the] act . . . simply because a coconspirator agreed to let him do so would produce an untenable construction of the statute and an unacceptable result.” Id. Moreover, like Chalavoutis, the defendant in Otuya made “arguments about [the AIT statute’s] purpose, history, and statutory titles” which the Fourth Circuit “rejected under an elementary rationale: [these arguments] cannot contradict a law’s plain text.” Id. at 190 (collecting cases). This Court finds the Fourth Circuit’s reasoning applicable and persuasive here.

This Court similarly does not find the consent of the person whose identity is used, whether a person is a “victim” in the practical sense or not, dispositive. See also Roberts-Rahim, 2015 WL 6438674 (the defendant’s family member allowed him to use

the family member's identification documents to fraudulently obtain a driver's license and passport for the defendant); United States v. Osuna-Alvarez, 788 F.3d 1183 (9th Cir. 2015) (the defendant's brother allowed him to use the brother's United States passport while smuggling drugs into the United States). Accordingly, Defendant's motion to dismiss Counts Six and Seven is DENIED.<sup>3</sup>

## II. Motion to Controvert the Search Warrant

Chalavoutis does not contest that there was sufficient probable cause for the warrant to issue. She argues that (1) the warrant, which fails to incorporate its supporting affidavit, is not particular, and (2) the warrant emerges from the wrong venue. (Def. Br. at 13, 18.)

### A. Particularity

At the outset, the Court does not consider Postal Inspector John Bizarro's affidavit "because it was neither incorporated in nor attached to the Search Warrant." United States v. Cwibeker, No. 12-CR-0632, 2014 WL 7423106, at \*4 (E.D.N.Y. Dec. 31, 2014) (noting that "because particularity deals with the extent to which the executing officer's discretion is cabined, the

---

<sup>3</sup> As this Court finds that the Straw Owner's apparent consent does not compel dismissal of the AIT counts, it need not review the grand jury minutes, as Defendant requests, "to determine the nature of the government's allegations regarding the issue of consent[.]" (Def. Br., at 11 n.4; see Def. Mot., ¶ 2.)

relevant perspective for that analysis is that of those at the scene of the search, who do not have meaningful access to the affidavit unless it is incorporated and attached") (internal quotation marks and citation omitted). As Defendant points out, the Government appears to concede that the affidavit was not incorporated, and rather argues that "[i]ncorporation . . . has no relevance here, because the warrant [itself] is sufficiently particular." (Gov't Opp. at 16.)

It is axiomatic that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. "Where the evidence, fruits, or instrumentalities to be seized are documents or computer data, the courts recognize the difficulties that the particularity requirement imposes on the Government, and have refused invitations to use those difficulties to render legitimate government investigations impotent." Cwibeker, 2014 WL 7423106 at \*5.

Here, the Court is mindful, and concerned, that the warrant commanded the email provider to turn over "the contents of all emails associated with the account" "from October 14, 2010 through December 6, 2016[.]" (Warrant at LC 000078.) However, "[s]uch a procedure is consistent with the well-established law of this Circuit." United States v. Robinson, No. 16-CR-0545, 2018 WL

5928120, at \*18 (E.D.N.Y. Nov. 13, 2018) (citing FED. R. CRIM. P. 41(e)(2)(B))<sup>4</sup> ("officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.")). "In the case of electronic evidence, which typically consists of enormous amounts of undifferentiated information and documents, courts have recognized that a search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search." In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxxx@gmail.com Maintained at Premises Controlled By Google, Inc. ("Google"), 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (collecting cases reflecting the difficulty and impracticality of conducting on-site searches and authorizing seizure of entire accounts, databases and systems for off-site searches).

Courts have applied the same analysis to email accounts as they have to hard drives. See Google, 33 F. Supp. 3d at 394 ("We perceive no constitutionally significant difference between

---

<sup>4</sup> The Advisory Committee notes to the 2009 amendments to Rule 41 explained the need for such a procedure: Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

the searches of hard drives just discussed and searches of email accounts. Indeed, in many cases, the data in an email account will be less expansive than the information that is typically contained on a hard drive."); Robinson, 2018 WL 5928120 at \*18 ("language in the Email Warrant authorizing the search for 'everything' in the Gmail Account" did not require suppression). The Google court noted that "every case of which we are aware that has entertained a suppression motion relating to the search of an email account has upheld the Government's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant." Google, 33 F. Supp. 3d at 394 (collecting cases).

Thus, despite its failure to incorporate the affidavit, this Warrant nonetheless conforms to warrants that have been consistently upheld in this Court and others. While it allowed a broad search of Defendant's email accounts, it limited the information to be seized by the Government in several ways: by reference to the crimes investigated, the participants, a time frame, and types of information and documents. The Court does not disagree with Defendant's contentions that these limitations did little to narrow the scope of the information to be seized: the time frame was six years, the participants included all unnamed co-conspirators, and the warrant allowed the seizure of any evidence indicating how and when Chalkvoutis' email account was

accessed or used. But under applicable law, the warrant passes muster.

1. The Good Faith Exception

However, even if this Court were to find the warrant lacks particularity, the good faith exception to the exclusionary rule applies. "As the Second Circuit has noted, 'suppression is our last resort, not our first impulse in dealing with violations of the Fourth Amendment.'" United States v. Shipp, 392 F. Supp. 3d 300, 312 (E.D.N.Y. 2019) (quoting United States v. Clark, 638 F.3d 89, 99 (2d Cir. 2011)) (further citation omitted). "Not every facially deficient warrant will be so defective that an officer will lack a reasonable basis for relying upon it" and "[t]hus, exclusion is appropriate only where a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." Cwibeker, 2014 WL 7423106 at \*8, \*7 (internal quotation marks, citations, and alteration omitted). "When an officer genuinely believes that he has obtained a valid warrant from a magistrate and executes that warrant in good faith, there is no conscious violation of the Fourth Amendment, and thus nothing to deter." Shipp, 392 F. Supp. 3d at 312 (internal quotation marks and citation omitted).

Even Shipp, a recent case relied upon by Defendant, held that "although the court has serious concerns about the breadth of the search authorized here and in similar cases, it nonetheless

finds that reliance on the Facebook Warrant by law enforcement officers was not objectively unreasonable. Application of the exclusionary rule in this case would thus serve little deterrent purpose.” Shipp, 393 F. Supp. 3d at 312. This Court shares those concerns. However, the Court cannot say that the law enforcement officers who relied upon this warrant, a type which is routinely upheld in this circuit and others, acted unreasonably in execution.

B. Venue

Chalavoutis next argues that “though an issue not yet decided by the Second Circuit, the Court should controvert the [W]arrant under Rule 41 because it granted search and seizure powers outside of the district of the issuing Magistrate.” (Def. Br. at 13.) She concedes, however, that other courts “addressing this issue have allowed for inter-jurisdictional warrants.” (Def. Br. at 19.) This Court agrees with the majority of those others and concludes that the Stored Communications Act (“SCA”) allows warrants for electronic communications to be issued by “a court of competent jurisdiction,” defined as including “any district court of the United States (including a magistrate judge of such a court) . . . that [ ] has jurisdiction over the offense being investigated[.]” 18 U.S.C. §§ 2703(a), 2711(3)(A)(i). This Court

has jurisdiction over the offenses investigated and charged here, and thus Magistrate Judge Shields properly issued the Warrant.

Courts have also specifically rejected Defendant's contention that the warrant violated the venue requirements of Federal Rule of Criminal Procedure 41(b). See United States v. Loera, 333 F. Supp. 3d 172, 189-190 (E.D.N.Y. 2018) (SCA's statement that warrant should be issued using the "procedures described in the Federal Rules of Criminal Procedure" is "more naturally read to refer to the process-related requirements" and not the venue requirements of Rule 41(b)) (noting "agree[ment] with other courts to consider this question"); United States v. Scully, 108 F. Supp. 3d 59, 83 (E.D.N.Y. 2015) (SCA Section "2703(a) authorizes electronic search warrants by a federal magistrate judge that extend outside his or her district.").

Additionally, even if Judge Shields' signing of the warrant violated any venue requirements, this Court would not find suppression to be an appropriate remedy, because "[a]ny lack of authority by the magistrate judge to issue the warrant has little

effect on police misconduct, which is the harm that suppression is designed to disincentivize.” Loera, 333 F. Supp. 3d at 190.

Accordingly, Defendant’s motion to convert the search warrant is DENIED in its entirety.

CONCLUSION

For the foregoing reasons, Defendant’s motion (D.E. 81) is DENIED in its entirety.

SO ORDERED.

\_\_\_\_\_  
/s/ JOANNA SEYBERT  
Joanna Seybert, U.S.D.J.

Dated: December 2, 2019  
Central Islip, New York